

# AN ERROR-CONTROL CODE WITH AN IMBALANCE OF ONES AND ZEROS TO PROVIDE A RESIDUAL CARRIER COMPONENT

E. R. Berlekamp  
Cyclotomics, Inc.

R. J. Currie  
Sperry Corporation

R. J. McEliece  
California Institute  
of Technology

C. K. Rushforth  
University of Utah

Po Tong  
Cyclotomics, Inc.

## ABSTRACT

We consider in this paper a direct sequence spread-spectrum communication system employing an error-control code having an imbalance of ones and zeroes. The primary motivation for using such a code is to provide a carrier component for synchronization as an alternative to the transmission of a separate pilot tone. We evaluate the performance of this system when a concatenated code whose inner code is a constant-weight subcode of the (24, 12) extended Golay code and whose outer code is a Reed-Solomon code. We consider the effects of both white Gaussian noise and burst jamming, and we evaluate several decoding algorithms with different complexities and different coding gains. Near-maximum-likelihood decoding can be realized at the lowest data rates of interest, while successively less complicated algorithms achieving corresponding smaller coding gains must be used as the data rate increases. The performance of this system compares favorably with that of a more conventional pilot-tone system.

## 1. INTRODUCTION

We consider in this paper an error-control scheme for a coherent spread-spectrum communication link that uses a phase-locked loop to achieve carrier synchronization. The most common method of providing the required carrier component to the receiver is to send a separate pilot tone. We propose and analyze an alternative scheme that uses an error-control code with an imbalance of ones and zeroes.

The advantages of concatenated codes using Reed-Solomon outer codes and either short block codes or short-constraint-length convolutional codes as inner codes are well documented [1], and such codes are widely used. The novel feature of our work is the required imbalance in the numbers of ones and zeroes in the codewords. Our approach to satisfying this requirement was to use as the inner code a short block code whose words have constant weight.

System synchronization requirements dictated a weight of between  $n/4$  and  $n/3$ , where  $n$  is the word length, while formatting and timing requirements led us to choose an overall code rate of one-fourth. The inner code we selected is a nonlinear code consisting of 128 words, each of length 22 and weight 7, derived from the extended Golay (24, 12) code. This code was developed by Tong [2] and will be described in a separate paper. The required overall rate is achieved by using as the outer code a shortened RS (126, 99) code.

The performance of the resulting concatenated code on the additive white Gaussian noise (AWGN) channel using several different decoding strategies is evaluated in Section 2. The effects of burst jamming are considered in Section 3.

We summarize our results and present our conclusions in Section 4. The essence of our conclusions is that the biased code described here achieves a performance comparable to that of a pilot-tone system with similar parameters [2], and thus represents an alternative that may be attractive in the face of overall system requirements. This code is currently being incorporated into a major data link.

## 2. PERFORMANCE ON THE AWGN CHANNEL

### 2.1 Maximum-Likelihood Decoding of Inner Code

Maximum-likelihood decoding of the inner code on the AWGN channel entails correlating the received signal with a set of stored reference signals, one corresponding to each word in the inner code, and selecting as the transmitted word that word yielding the largest correlation. For definiteness, we take the data modulation to be BPSK, and we assume perfect synchronization. The probability of decoding the inner code incorrectly depends on the details of the distance structure, which is complicated. We obtain an approximation to this error probability using the tangential union bound described in [1], a bound believed to be tight.

The possible distances between codewords in the Golay (24, 12) code are 8, 12, 16, and 24. Words at distance 8 from the transmitted word are the dominant sources of error, of course, and we neglect the contributions of those words at greater distances. In our purged and shortened inner code, there are on the average 78.75 codewords at distance 8 from each codeword. Application of the tangential union bound developed in [1] yields as an approximation to the word error probability of the inner code:

$$q = \int_{-\infty}^{\infty} A_D f \left[ \left( \sqrt{nE_s} - t \right) \sqrt{D/(n-D)} \right] \cdot \frac{1}{\sqrt{2\pi}} e^{-t^2/2} dt + f(z) \quad (1)$$

where  $D$  is the minimum distance,  $E_s$  is the symbol energy,  $n$  is the word length,  $A_D$  is the average number of words at minimum distance from a given word, and

$$f(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-u^2/2} du \quad (2)$$

The parameter  $x$  is determined implicitly by the equation

$$f(x) = \sqrt{\frac{n}{2}} \left( 1 - \frac{1}{A_D} \right) = \frac{1}{A_D} \quad (3)$$

For our inner code we have  $n = 22$ ,  $D = 8$ , and  $A_D = 78.75$ . A plot of the word error probability  $q$  from (1) using these parameters is shown in Fig. 1. The abscissa is  $E_b/N_o$ , where  $E_b$  is the energy per bit and is related to  $E_s$  by

$$E_b = \frac{22}{7} E_s \quad (4)$$

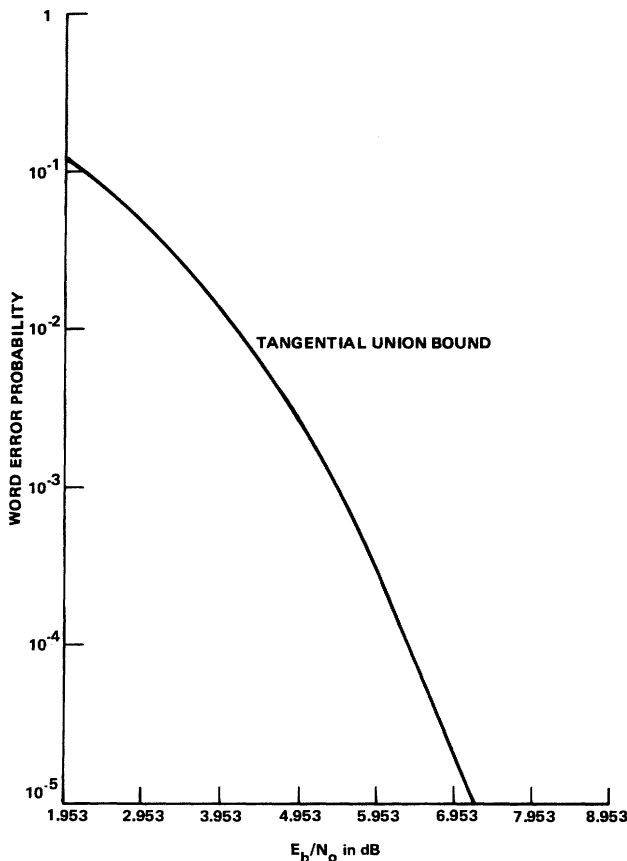


Figure 1. Performance of inner code with maximum likelihood decoding.

## 2.2 Performance of Concatenated Code

The concatenated code whose performance is to be evaluated here has the purged and shortened Golay code described in the previous subsection as its inner code and a Reed-Solomon (126, 99) code as its outer code. We now evaluate the performance of this concatenated code on the AWGN channel assuming maximum-likelihood decoding of the inner code and errors-only decoding of the outer code using the full available redundancy of 27 symbols. We will consider other decoding strategies in Section 2.3.

The bit error probability of the concatenated code is given by [1]

$$P_b = \sum_{t=0}^{\left\lfloor \frac{x}{2} \right\rfloor + 1} \binom{126}{t} \left( \frac{64}{127} \right)^t \left( \frac{1}{126} \right)^{126-t} q^t (1-q)^{126-t} \quad (5)$$

where  $r$  is the number of redundant symbols (27 in the present case),  $q$  is the word error probability of the inner code as determined in Section 2.1, and  $[x]$  is the largest integer less than or equal to  $x$ . A plot of  $P_b$  versus  $E_b/N_o$  is shown in Fig. 2. Note that  $E_b = 4E_s$  since the overall rate is one fourth. The coding gain at  $P_b = 10^{-6}$  relative to uncoded transmission is approximately 6.1 dB.

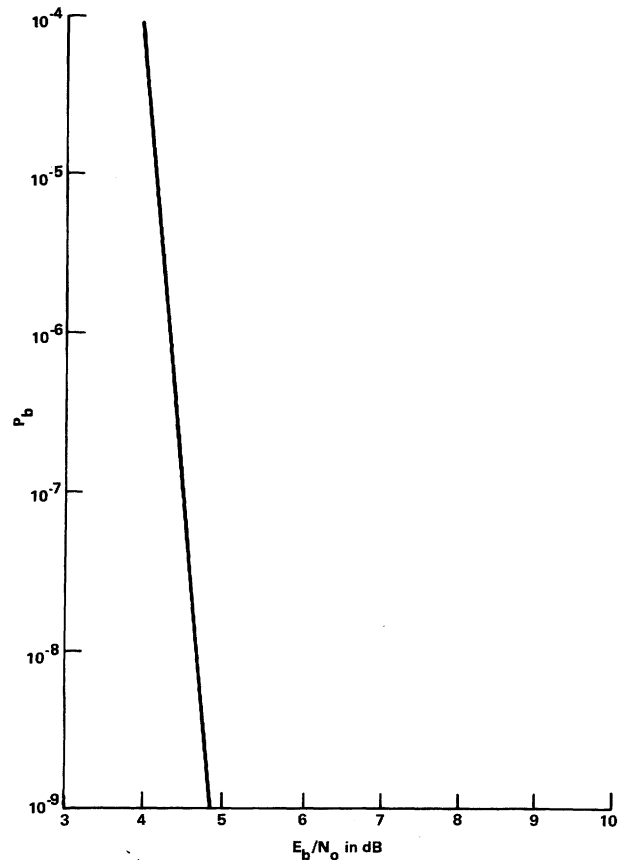


Figure 2. Performance of concatenated code with ML decoding of inner code.

## 2.3 Other Decoding Strategies

The coding scheme we are considering can be adapted to a variety of data rates by changing the decoding strategy. Full maximum likelihood decoding as described above can be accomplished at modest data rates, but simpler strategies must be used as the data rates increase to tens or hundreds of megabits. We have considered the following five strategies for decoding the inner code:

- Strategy 1: All error patterns of weight 3 or less are corrected; all patterns of weight 4 and many patterns of weight 5 or more are detected and reported as erasures to the outer code.
- Strategy 2: The least reliable bit is changed, if necessary, in order to make the number of errors odd. Error patterns of weight 3 or less are corrected, there is no error detection.
- Strategy 3: The same as Strategy 2, except that most patterns of weight 5 or greater are detected and reported as erasures to the outer code.
- Strategy 4: The least reliable bit is changed, if necessary, to make the number of errors even. Then error patterns of weight 2 are corrected, error patterns of weight 4 are scored and decoded by maximum likelihood decoding, and most error patterns of weight 6 or more are detected and reported to the outer code as erasures.
- Strategy 5: Maximum likelihood decoding.

The outer code will use errors-only decoding or errors-and-erasures decoding as appropriate. Moreover, we consider as an additional decoding option the utilization of only a portion of the available redundancy in the outer code in order to reduce the computational burden still further.

We omit the performance calculations for these strategies in the interest of brevity and simply summarize the results in Table 1. This table shows the coding gains achieved at  $P_b = 10^{-6}$  for the decoding strategies described above and for various amounts of redundancy utilized in the process of decoding the outer code. The various strategies included in this performance matrix provide a wide range of complexities and coding gains. The relatively high gains in the lower right portion of the matrix can be achieved at moderate data rates, while the less complex but less powerful strategies in the upper left portion might be appropriate at very high rates (many tens of megabits).

**Table 1. Coding Gains, in dB, for various decoding strategies.**

	Outer Code Redundancy				
	$r = 2$	$r = 4$	$r = 8$	$r = 16$	$r = 27$
Strategy 1	1.1	1.8	2.7	3.6	4.4
Strategy 2	1.3	2.0	2.7	3.5	4.1
Strategy 3	1.5	2.3	3.2	4.1	5.0
Strategy 4	2.5	3.3	4.2	5.0	5.6
Strategy 5	3.2	3.9	4.7	5.5	6.1

### 3. PERFORMANCE AGAINST A BURST JAMMER

For the purpose of these performance evaluations, we assume that background additive white Gaussian noise with power spectral density  $N_0/2$  is present. In addition, a given symbol is erased with probability  $e$ , the erasures being independent from symbol to symbol. In effect, we have assumed ideal interleaving and perfect detection of the presence of the jammer. As before, we assume BPSK modulation with a symbol energy of  $E_s$ .

Consider two codewords which differ from each other in  $\omega$  positions. The probability that  $i$  erasures will occur among these  $\omega$  positions is

$$q_i = \binom{\omega}{i} e^i (1 - e)^{\omega - i} \quad (6)$$

When maximum-likelihood decoding of the unerased portion of the word (i.e., correlation detection with erased positions blanked out) is used, the probability of mistaking one word for the other, given that  $i$  of the  $\omega$  distinguishing symbols have been erased, is

$$p_i = f \left[ \sqrt{\frac{2(\omega - i) E_s}{N_0}} \right] \quad (7)$$

where  $f(\cdot)$  is defined in (2).

Averaging over  $i$ , we find the pairwise error probability between words differing in  $\omega$  positions to be

$$P_\omega = \sum_{i=0}^{\omega} \binom{\omega}{i} e^i (1 - e)^{\omega - i} f \left[ \sqrt{\frac{2(\omega - i) E_s}{N_0}} \right] \quad (8)$$

Further improvements in performance can be achieved at low data rates by incorporating time diversity. Each symbol is partitioned into  $d$  chips, each having energy  $E_s/d$ . Thus, the energy per code symbol remains the same. Interleaving is performed at the chip level, leading to a situation in which chips erased independently with probability  $e$ .

Codewords differing in  $\omega$  code symbols will differ in  $d\omega$  chips when a diversity of  $d$  chips per symbol is used, and (8) becomes:

$$P_\omega = \sum_{i=0}^{d\omega} \binom{d\omega}{i} e^i (1 - e)^{d\omega - i} f \left[ \sqrt{\frac{2(d\omega - i) E_c}{N_0}} \right] \quad (9)$$

where

$$E_c = \frac{E_s}{d} \quad (10)$$

is the energy per chip.

Overall performance calculations now proceed much as before. The pairwise error probabilities given by (8) or (9) can be used in conjunction with the union bound or the improved tangential union bound to obtain an estimate of the word error probability for the inner code. This quantity then becomes the symbol error probability in calculating the bit error probability of the outer Reed-Solomon code.

A plot of  $P_b$  versus  $E_b/N_0$  for various values of the erasure probability  $e$  and no diversity ( $d = 1$ ) is shown in Fig. 3. Also shown for comparison is the curve for uncoded BPSK. The gain due to diversity is illustrated in Fig. 4, which is similar to Fig. 3 except that the diversity  $d$  is equal to 4. The gain due to diversity at  $e = 0.2$  is about 0.5 dB.

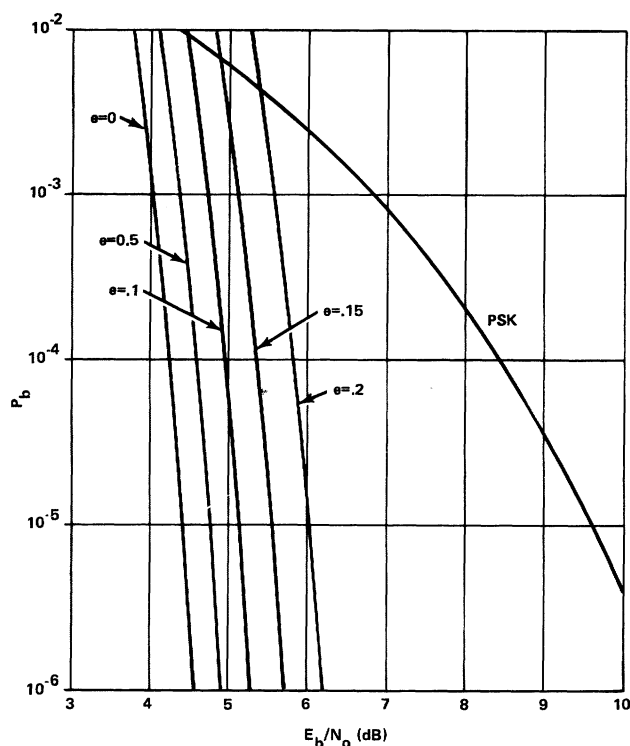


Figure 3. Performance against burst jammer, no diversity.

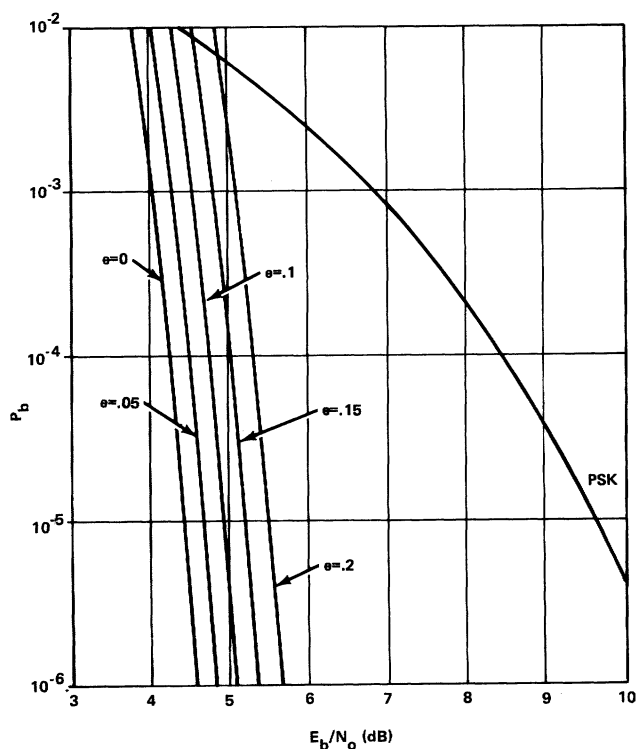


Figure 4. Performance against burst jammer,  $d = 4$ .

## 5. SUMMARY AND CONCLUSIONS

We have considered in this paper an error-control code designed to have an imbalance of ones and zeroes for the purpose of creating a carrier component to be used in synchronization. We have evaluated the performance of this code on the AWGN channel and in the presence of burst jamming for a wide variety of decoding strategies. The performance achieved by this system is generally comparable to that achieved by a pilot-tone system with comparable parameters when the energy required by the pilot tone is taken into account [2], but the unbalanced code may have certain implementation advantages. This code is currently being incorporated in a major data link.

## REFERENCES

1. E. R. Berlekamp, "The Technology of Error-Correcting Codes," Proceedings of IEEE, Vol. 68, No. 5, May 1980, pp. 564-593.
2. Cyclotomics, Inc., Final Report on Biased Code Study, prepared for Sperry Corporation, January 28, 1983.